ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

A Comparative Analysis on Various Intrusion Detection Techniques for Wireless Sensor Networks

C.Anuradha, Sundararajan.M, Arulselvi S

Assistant Professor, Department of Computer Science, Bharath University, Chennai, Tamil Nadu, India

Director, Research Center for Computing and Communication, Bharath University, Chennai, Tamil Nadu, India

Co-Director, Research Center for Computing and Communication, Bharath University, Tamil Nadu, India

ABSTRACT: Wireless sensor networks have sensor nodes which can process the input data from attached sensor s. The results are transmitted wirelessly to the transit network. Large number of applications are widely benifited from such networks making it vulnerable to threats. It is becoming a growing area for research and development as wireless sensor networks are used in military, surveillance, etc. Security for WSNs are very important as the nodes are not physically protected. In this paper, we analyse the various security threats available for WSNs. In this paper, a novel technique for providing faced by WSNs.

KEYWORDS: cluster, cluster-head, clique, MUSK architecture

I. INTRODUCTION

Wireless sensor networks (WSN) have become increasingly one of the most promising and interesting areas over the past few years. These networks may be very large systems comprised of small sized, low power, low-cost sensor devices that collect detailed information about the physical environment. Each device has one or more sensors, embedded processor , and low-power radio and is normally battery operated. Examining each such single device individually, might appear to have small utility. Different types of network topologies such as star, tree, mesh etc are used for communication in WSN. Intrusion is characterized as a set of actions that leads to either an unauthorized access or an alteration of the existing system. An Intrusion Detection System (IDS) is a dynamic monitoring system used to identify, examine and observe violated activities. It discovers breach and illegal access to confidentiality, unavailability, authorization, authentication, integrity and network resources In a cluster based hierarchical approach, concentration of sensor nodes forms a cluster and one node among them acts as a Cluster Head and is normally denoted as CH. It is assumed to have a larger battery and acts as a supervisor node for communication between other nodes. All CH in the network are connected to a Base Station (BS) which is a single decision making authority as shown in the following figure 1.

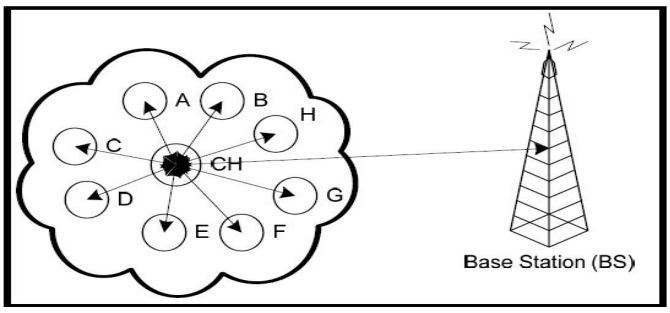

Figure 1

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

There are various protocols for intrusion detection system in WSN. This paper analyses several existing protocols that are currently being used for IDS in WSN. Also it proposes a new technique used for intrusion detection in WSN.

II. SECURITY ISSUES

The following are the security threats available to the wireless sensor networks.

2.1 Routing Threats

The simplicity of many routing protocols for WSN make them a easy target for attacks. Karlof and Wagner in a paper classify the routing attacks into the following categories:

1.Spoofed, altered, or replayed routing information :

While sending the data, the information in transit may be altered, spoofed, replayed, or destroyed. Since sensor nodes have only short range transmission, an attacker with high processing power and larger communication range could attack several sensors simultaneously and the transmitted information may be modified.

2. Selective forwarding

In this kind of attack a malicious node may refuse to forward every message it gets, acting as a black hole or it can forward some messages to the wrong receiver and simply drop others.

3. Sinkhole attacks

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the malicious node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus
route with the shortest path to the requested destination.

4. Sybil attacks

In Sybil attack the compromised node presents itself as it is multiple nodes. This type of attack tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection.

5. Wormholes

Wormhole attack is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn't exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

6. HELLO flood attacks

This attack is based on the use by many protocols of broadcast Hello messages to announce themselves in the network. So an attacker with greater range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

7. Acknowledgement

Some wireless sensor network routing algorithms require link layer acknowledgements. A compromised node may exploit this by spoofing these acknowledgements, thus convincing the sender that a weak link is strong or an dead sensor is alive.

III. PROPOSED SCHEME

3.1. Formation of Cluster-Head

In our model, we have used a technique to create the clusters as mentioned in [1][2] which is called Cluster-First, secure and distributed cluster formation protocol. Each of the cluster will have a separate cluster-head(CH). When all the nodes need to send data to a distant base station, energy consumed will be very high. So when we use cluster-first protocol, it will reduce the energy consumed in transmitting data. By exchanging information with 1-hop neighbors, normal sensor nodes are divided into mutually disjoint cliques, in which all the nodes can directly communicate with each other. This protocol guarantees that all the normal nodes in each clique agree on the same clique membership under the attacks from both external and internal malicious nodes. When this protocol is used, malicious nodes can be distinguished from normal nodes when their behaviours do not sink with the normal ones. Also it helps in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

removing inside attackers that deviate from the protocol. The protocol uses four steps in creating clusters. When an inconsistency is detected, an extra fifth step is used whisc explained as follows.

1. Each node computes its local maximum clique after
exchanging neighbour lists with its neighbour.
2. Each node exchanges its neighbour list with its neighbour, compares its local maximum clique with that of neighbour and updates its local maximum clique.
3. The updated clique is exchanged between neighbours and the final clique is derived.
4. The derived final clique value is passed between the neighbours. If no inconsistency is detected, it terminates successfully.
5. If any inconsistency is detected, it removes the malicious nodes from the network and it is restarted.

Malicious nodes may employ different methods to compromise clique agreement among normal nodes. Our protocol can prevent external attacks by using (unicast and broadcast) message authentication. Thus, a malicious node cannot use a fake identity in the above described protocol without grasping the keying materials. If malicious nodes broadcast the same false messages or keep silence to all the normal neighbors, they cannot introduce clique inconsistency. Malicious nodes may send inconsistent messages in different steps. Since such attacks generate the same impact on all the normal neighbors, they cannot introduce clique inconsistency either. Therefore, clique inconsistency only results from sending different messages to different normal nodes, or launching silence attacks from malicious nodes.

3.2. IDS for Clustering-based Sensor Networks

Su, et al. [5][4] propose two approaches to improve the security of cluster-based sensor networks using intrusion detection systems. The first approach use a model based on authentication, which can only resist outside attackers. Its basic technique is to append a message authentication code (MAC) to every message. Each time a node wants to send a message it appends to it a time stamp and a MAC is generated by the pairwise key or individual key depending on the role of the sender (cluster-head, member-node, or base
station. An another scheme called Energy-Saving offers protection against outside attackers. This approach focuses on detecting misbehavior both in member-nodes (MN) and in cluster-head nodes (CH). Member-nodes are monitored by cluster-head node since every MN sends its data to its CH. When a misbehavior is detected the CH broadcasts an alarm
message encrypted with the cluster key to restrain this specific node. CH monitoring is done with the following algorithm. First the CH decides which nodes are energy capable of monitoring the CH. This is achieved by sending messages querying the energy state of every MN. CH ignores the nodes with low energy and divides the remaining MNs into groups. Every group then monitors the CH in turn. At
any moment only one group (the active group) is monitoring the CH. When a misbehavior is detected at least by X monitor nodes, then the CH is revoked.

3.3. Intrusion Detection System

We have used Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS) proposed by [5][6] which provides two tiers of security in WSN. In order to provide two tiers of security we have installed Musk architecture [6][7] on each Cluster Head (CH). We have modified the MUSK architecture in order to behave as mobile agent. This architecture works as the Network Intrusion Detection System (NIDS) as well as Local Intrusion Detection System (LIDS) on WSN. We have used two threshold frequencies. The threshold 1 is set on each CH for the normal activity of the network and threshold 2 is set on each sensor node for its normal activity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

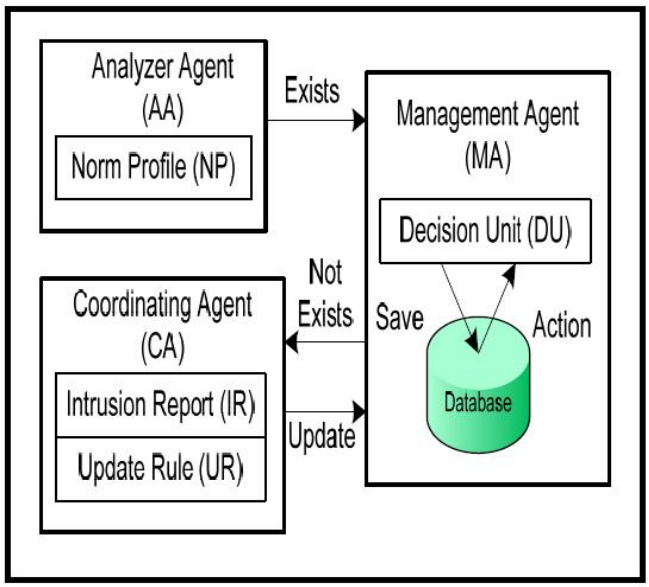

Fig. 2 MUSK Architecture [6]

NIDS: The different agents of Musk architecture [25] works as NIDS which is installed on each Cluster Head (CH) within a network. The NIDS capture the data packets along the path to identify an intrusion activity. The modified form of Musk architecture is shown in the Fig.2. This architecture is comprises of three agents: Analyzer Agent (AA), Coordinating Agent (CA) and Management Agent (MA). When the CH detects an intrusion it sends a copy of Analyzer agent (AA) to the victim node. Therefore AA is mobile in nature. The CA and MA are preset in the CH and they are fixed.

Analyzer Agent (AA): The Analyzer Agent (AA) is used to monitor node activity. It is a mobile agent and installed on each CH in the network. When CH discovers an intrusion it sends a copy of AA to the suspicious node. The AA uses victim resources in order to verify the occurrences of intrusion. The AA generates a Norm Profile (NP) and check the threshold 2. If there is a deviation from the threshold frequency the AA generates an alarm and notifies the CH. The CH calls the Management Agent (MA) for analysis.

Management Agent (MA): The Management Agent (MA) contains a sub unit called Decision Unit (DU) for the analysis of intrusion. The DU maintains the database of already occurred intrusions. When an intrusion occurs the CH calls the MA for analysis. The MA activates its DU that searches in its database whether this intrusion happens in the past or not. The database contains the predefined stored intrusions along with the decisions. If the match occurs against the pre stored intrusions then DU performs already stored decision and informs to the CH. If there is no such entry in the database then MA informs the Co-ordinating Agent (CA) regarding the occurrence of novel intrusion.

Coordinating Agent (CA): The Coordinating Agent (CA) performs two basic functions i.e. generate Intrusion Report (IR) and Update Rule (UR). When CA receives a novel intrusion message from MA it sends to IR. The IR forwards this report to the Base Station (BS) regarding the occurrence of intrusion. The BS is a centralized decision making authority against the intrusion. It makes a decision on novel intrusion and sends it to the Update Unit (UU). The UU generates new rule against that intrusion and send it to MA. The MA saves the intrusion in the database for future use. If the same intrusion happens again the DU searches the database and performs the already stored decision.

LIDS: The Analyzer Agent (AA) is a mobile agent and works as LIDS. When NIDS in CH deviate from its threshold 1 it generate an alarm informing the occurrence of intrusion. The CH makes analysis and identifies the sensor node that is generating abnormal traffic. The CH activates its mobile AA and send to the victim node. The AA works as LIDS and uses resources of the suspicious node for identifying the malicious activities. The AA informs the CH either the suspicious node is victim or safe. If the node is victim the CH that takes appropriate action upon that activity. The copy of AA is only send to the suspicious node instead of installing LIDS on each sensor node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

3.4. Working Paradigm

We set two threshold levels for intrusion detection, one for Network Intrusion Detection System (NIDS) and other for Local Intrusion Detection System (LIDS). Threshold 1 is set
on each CH over the network and works as the NIDS whereas the threshold 2 is set on each sensor node and works as LIDS. The initial intrusion detection is performed by NIDS which detects the normal rate of packet arrival and departure. In case of deviation from threshold 1, the CH triggers the mobile Analyzer Agent (AA) over the link where deviation is occurred.

The AA will visit the suspicious node and acts as Local Intrusion Detector (LID) over there. The AA will use the resources of suspicious node to investigate its behavior further. This investigation is based on threshold 2. If suspicious node is found the victim the AA will update CH. The CH inform its sub agents i.e. Coordinating Agent (CA) and Management Agent (MA) that will take appropriate action to prevent rest of the network from intrusion either by minimizing the communication with the victim node, reducing the trust value on the victim node or by cutting its communication from rest of the network. Otherwise, the AA informs the CH that the suspicious node is not the victim; it is a safe node and unusual but harmless activity has taken place.

V.ADVANTAGES

The Major advantage our proposed approach is that it provides two levels of security by using resources of sensor network optimally. It also reduces the workload of Cluster Head (CH) and provides enhanced security. As in existing schemes CH is responsible for all computation pertaining to the intrusion detection activity in member nodes of the CH. Whereas in our proposed scheme CH triggers the AA for suspicious node on its every unusual activity. The AA uses suspicious node's resources in order to declare it either as a victim or safe node. In this way CH resources are saved as compared to the existing schemes. Another benefit of our approach is infrastructural reduction as we do not need to install LIDS on every node rather mobile agent acts as a LIDS on suspicious node. This enhances the overall life time of the sensor network.

VI. CONCLUSIONS

The resource restricted nature of WSN demands a more sophisticated and secure security mechanism for these sorts of networks. There seems an inverse relationship in better security and optimum resource utilization of network resources in existing security schemes of WSN. In this research article, we have proposed a security model which not only provides good level of security but it also uses network resources optimally for the provision of better security. In proposed approach, we have proposed a two tier security model for WSN. The NIDS and LIDS are involved in providing two tier securities. The NIDS is installed on all CH whereas LIDS is based on mobile agent. The LIDS is activated whenever CH found any node suspicious. The CH issues LIDS for further scrutiny of malicious activities of suspicious node in order to affirm it as a compromised node. The LIDS uses resources of suspicious node. So the proposed scheme provides better security against intrusions in WSNs.

REFERENCES

[1] K. Sun, P. Peng, P. Ning, and C. Wang, "Secure Distributed Cluster Formation in Wireless Sensor Networks", in Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC' 06), Pages: 131-140, December 2006.
[2] Kaliyamurthie K.P., Parameswari D., Udayakumar R., "QOS aware privacy preserving location monitoring in wireless sensor network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4648-4652.
[3] Ourstou D., Matzner S., Stump W., Hopkins B., and Richards K., "Identifying Coordinated Internet Attacks", Proceedings of the Second SSGRR Conference. Rome, Italy, 2001.
[4] Shirley Gloria D.K., Immanuel B., Rangarajan K., "Parallel context-free string-token petri nets", International Journal of Pure and Applied Mathematics, ISSN : 1311-8080, 59(3) (2010) pp.275-289.
[5] Park H.J. and Cho S.B., "Privilege Flows Modeling for Effective Intrusion Detection based on HMM", Department of Computer-Science,Yonsei University, Seoul 120-749, Korea.
[6] Ramakrishnan V., Srivatsa S.K., "Pitch control of wind turbine generator by using new mechanism", Journal of Electrical Systems, ISSN : 1112-5209, 6(1) (2010) pp.1-15.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

[7] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.- F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wirelss for the Masses - Ready for Take-off, Mar 13-17 2005.
[6] Karthikeyan T., Subramaniam R.K., Johnson W.M.S., Prabhu K., 'Placental thickness & its correlation to gestational age & foetal growth parameters-a cross sectional ultrasonographic study", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(10) (2012) pp.1732-1735.
[7] Surraya Khanum, Muhammad Usman and Ala'a Alwabel , "Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks", in jan 2012 IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3.
[8] Sathish Kumar M., Karrunakaran C.M., Vikram M., "Process facilitated enhancement of lipase production from germinated maize oil in Bacillus spp. using various feeding strategies", Australian Journal of Basic and Applied Sciences, ISSN : 1991-8178, 4(10) (2010) pp. 4958-4961.
[9] S. Khanum, M. Usman, K. Hussain, R. Zafar, and Dr M. Sher, "Energy-Efficient Intrusion Detection System for Wireless Sensor Network Based on MUSK Architecture" HPCA 2009, LNCS 5938, pp. 212–217, Springer- Verlag Berlin Heidelberg 2010
[10] L. Eschenauer and V. D. Gligor, "A keymanagement scheme for distributed sensor networks", Proceedings of the 9th ACM conference on Computer and communications security, November 18-22, 2002, Washington, DC, USA
[11] A. Perrig, J. Stankovic, and D.Wagner, "Security in wireless sensor networks", Communications of the ACM, Volume 47 , Issue 6 (June 2004)
[12] A.S.K. Pathan, H-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges", Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, Vol.2, Iss., 20-22 Feb. 2006
[13] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", In Proc. of First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
[14] A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks", communications of the ACM, vol. 47, no. 6, June 2004.
[15] Y. Wei, L. Paul and J.M. Havinga, "How to Secure a Wireless Sensor Network", Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Netherlands, Published by IEEE ISSNIP, 2005.
[16] T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks" School of Information Technologies, University of Sydney, Published by IEEE, 2007.
[17] H. Debar, D. Curry, and B. Feinstein, "The Intrusion Detection Message Exchange Format", draft-ietf-idwg-idmef-xml-14 (Work in Progress), January 2005.
[18] S. Zhu, S. Setia, and S. Jajodia, LEAP: "Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C.,
October 2003.
[19] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami. (2006) "Intrusion detection for routing attacks in sensor networks," International Journal of Distributed
Sensor Networks, Vol 2, pp. 313–332.
[20] Wei-Tsung Su, Ko-Ming Chang, and Yau-Hwang Kuo. Ehip, (2007) "An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks," Computer
Networks, Vol 51, pp. 1151–1168.
[21] Ioannis Krontiris, Tassos Dimitriou, and Felix C. Freiling. (2007) "Towards intrusion detection in wireless sensor networks," *In Proceedings of the 13th European Wireless Conference*.
[22] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos. (2008) "Intrusion detection of sinkhole attacks in wireless sensor networks. In Algorithmic Aspects of
Wireless Sensor Networks," Vol 4837, pp. 150–161. Springer Berlin / Heidelberg.
[23] Fang Liu, Xiuzhen Cheng, and Dechang Chen, (2007) "Insider attacker detection in wireless sensor networks," In INFOCOM 2007. *26th IEEE International Conference on Computer Communications. IEEE*, pp. 1937–1945.
[24] J.Arul Hency Sheela, GC-MS Studies of the Plant Clematis Gouriana , International Journal of Innovative Research in Science, Engineering and Technology , ISSN: 2319-8753 ,pp 13514-13519 ,Vol. 3, Issue 6, June 2014.
[25] Jemima Daniel,Usage of Language,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753, pp 7073-7075,Vol. 2, Issue 12, December 2013.
[26] Jemima Daniel,The Duality of Human Nature,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 511-512,Vol. 2, Issue 2, February 2013.
[27] Jemima Daniel,Impact of E-Mail communication,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 527-528,Vol. 2, Issue 2, February 2013.
[28] Jemima Daniel,The Enchanting World In Karnas`S Plays,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 757-758,Vol. 2, Issue 3, March 2013.
[29] Jemima Daniel,Myth in Indian English Dramas,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 1551-1555,Vol. 2, Issue 5, May 2013.